

Oracle® Cloud

Amministrazione del controllo dell'accesso per Oracle Enterprise
Performance Management Cloud

F28914-05

Oracle Cloud Amministrazione del controllo dell'accesso per Oracle Enterprise Performance Management Cloud

F28914-05

Copyright © 2015-, 2021, Oracle e/o relative consociate.

Autore principale: EPM Information Development Team

Sommario

Accesso facilitato alla documentazione	v
Feedback relativi alla documentazione	vii
1 Panoramica di Controllo accesso	
Informazioni su questa guida	1-1
Apertura di Controllo accesso	1-2
Gestione di gruppi	1-2
Creazione di gruppi	1-3
Modifica di gruppi	1-4
Eliminazione di gruppi.....	1-5
Importazione delle assegnazioni di utenti a un gruppo da un file	1-5
Assegnazione di un utente a molti gruppi.....	1-6
Utilizzo della ricerca.....	1-7
2 Gestione dell'assegnazione dei ruoli a livello di applicazione	
Ruoli delle applicazioni Planning e Consolidation.....	2-2
Ruoli dell'applicazione Oracle Enterprise Data Management Cloud	2-3
Assegnazione di ruoli a un gruppo o a un utente.....	2-4
Rimozione di ruoli a livello di applicazione assegnati a un gruppo o a un utente.....	2-5
3 Generazione di report	
Generazione di un Report assegnazioni ruoli per un utente o un gruppo	3-1
Visualizzazione del Report assegnazioni ruoli per l'ambiente in uso	3-2
Visualizzazione del Report accesso utenti	3-3
Visualizzazione ed esportazione del Report gruppo utenti.....	3-4

Accesso facilitato alla documentazione

Per informazioni sull'impegno di Oracle riguardo l'accesso facilitato, visitare il sito Web Oracle Accessibility Program all'indirizzo <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accesso al Supporto Oracle

I clienti Oracle che hanno acquistato il servizio di supporto tecnico hanno accesso al supporto elettronico attraverso My Oracle Support. Per informazioni, visitare <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oppure <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> per clienti non utenti.

Feedback relativi alla documentazione

Per fornire un feedback su questa documentazione, fare clic sul pulsante Feedback in fondo alla pagina in un qualsiasi argomento di Oracle Help Center. È inoltre possibile inviare un messaggio e-mail a epmdoc_ww@oracle.com.

Panoramica di Controllo accesso

L'accesso ai componenti di Oracle Enterprise Performance Management Cloud è controllato dai ruoli predefiniti nel dominio di Identity al quale sono assegnati gli utenti. Gli amministratori servizi possono assegnare agli utenti ruoli specifici delle applicazioni Planning, Consolidation e Data Management per consentire loro di eseguire task aggiuntivi in un ambiente.

Ad esempio, gli amministratori servizi possono assegnare a un utente il ruolo di Amministratore approvazioni di un'applicazione Planning o Consolidation per consentire all'utente di svolgere attività correlate alle approvazioni.

Inoltre, gli utenti con ruolo Amministratore servizi possono utilizzare Controllo accesso per creare gruppi composti da utenti o da altri gruppi del dominio di Identity. L'assegnazione di ruoli a questi gruppi consente agli amministratori servizi di concedere i ruoli a più utenti contemporaneamente, riducendo di conseguenza i costi amministrativi.

L'assegnazione di ruoli a livello di applicazione consente di migliorare solo i diritti di accesso degli utenti. Nessuno dei privilegi concessi da un ruolo predefinito può essere ridimensionato da ruoli assegnati a livello di applicazione.

Controllo accesso consente di completare le seguenti attività in un ambiente.

- [Gestione di gruppi](#)
- [Assegnazione di ruoli a un gruppo o a un utente](#)
- [Generazione di un Report assegnazioni ruoli per un utente o un gruppo](#)
- [Visualizzazione del Report assegnazioni ruoli per l'ambiente in uso](#)
- [Visualizzazione del Report accesso utenti](#)

Informazioni su questa guida

Controllo accesso si applica ai processi aziendali di Oracle Enterprise Performance Management Cloud elencati di seguito.


- Planning
- Moduli di Planning
- Consolidamento finanziario e chiusura
- Tax Reporting
- Profitability and Cost Management
- Account Reconciliation

- Oracle Enterprise Data Management Cloud
- Narrative Reporting
- Oracle Strategic Workforce Planning Cloud
- Oracle Sales Planning Cloud

Apertura di Controllo accesso

Per l'assegnazione dei ruoli specifici di applicazione a gruppi e utenti, si utilizza **Controllo accesso**, disponibile nella scheda **Strumenti** della home page.

Per aprire Controllo accesso, procedere come segue.

1. Accedere all'ambiente come amministratore dei servizi.
2. Eseguire uno dei passi indicati di seguito.
 - Fare clic su  (Navigator), quindi su **Controllo accesso**.
 - Fare clic su **Strumenti** e quindi su **Controllo accesso**.
 - Solo **Oracle Enterprise Data Management Cloud e Narrative Reporting**: fare clic su **Controllo accesso**.

Gestione di gruppi

Oracle Enterprise Performance Management Cloud utilizza un repository interno per supportare le assegnazioni di ruoli a livello di applicazione e memorizzare le informazioni sui gruppi utilizzati durante il processo di assegnazione dei ruoli.

Gli utenti di EPM Cloud e gli altri gruppi possono essere membri di gruppi gestiti tramite Controllo accesso. È possibile concedere ruoli applicazione agli utenti mediante l'assegnazione di un ruolo al gruppo.

Per consentire la visualizzazione delle assegnazioni utente, in Controllo accesso i ruoli predefiniti sono elencati come gruppi. Non è possibile assegnare loro ruoli o modificarne i ruoli da Controllo accesso. Inoltre, gli utenti EPM Cloud assegnati a ruoli predefiniti sono elencati in Controllo accesso in modo da poter essere aggiunti come membri di gruppo. Fare riferimento alla sezione Introduzione ai ruoli predefiniti in *Guida introduttiva a Oracle Enterprise Performance Management Cloud per gli amministratori*.

- [Creazione di gruppi](#)
- [Modifica di gruppi](#)
- [Eliminazione di gruppi](#)

Nota: Non è possibile utilizzare Controllo accesso per importare informazioni sui gruppi da un file allo scopo di creare dei gruppi. Analogamente, non è possibile esportare le informazioni sui gruppi mediante Controllo accesso. Per importare i gruppi è possibile utilizzare Migrazione o il comando createGroups di EPM Automate.

Creazione di gruppi

Solo gli amministratori del servizio possono creare e gestire i gruppi. Gli utenti di Oracle Enterprise Performance Management Cloud e altri gruppi possono essere membri di un gruppo.

Nota: È inoltre possibile utilizzare Migrazione o il comando createGroups di EPM Automate per importare da un file le informazioni sui gruppi allo scopo di creare gruppi.

Per creare i gruppi, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento alla sezione [Apertura di Controllo accesso](#).
2. In **Gestione gruppi**, fare clic su **Crea**.
3. In **Crea gruppo**, procedere come segue.
 - a. Nel campo **Nome** immettere un nome di gruppo (massimo 256 caratteri).

Per i nomi gruppo non è prevista la distinzione tra maiuscole e minuscole. Per evitare ambiguità nei report di sicurezza, EPM Cloud non consente di creare gruppi con nomi identici ai nomi di ruolo correnti e definiti in precedenza (Amministratore servizi, Utente avanzato, Utente, Visualizzatore, Responsabile pianificazione, Amministratore di sistema, Amministratore applicazione, Amministratore librerie, Amministratore di report).
 - b. **Facoltativo:** immettere una descrizione del gruppo.
4. **Facoltativo:** aggiungere gruppi per creare un gruppo nidificato.
 - a. In **Gruppi disponibili**, cercare i gruppi. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

I gruppi che soddisfano il criterio di ricerca vengono elencati in **Gruppi disponibili**.
 - b. In **Gruppi disponibili**, selezionare i gruppi membri del nuovo gruppo.
 - c. Fare clic su **Sposta**.

I gruppi selezionati sono riportati in **Gruppi assegnati**. Per rimuovere i gruppi assegnati, selezionare il gruppo da rimuovere in **Gruppi assegnati**, quindi fare clic su **Rimuovi**.
5. **Facoltativo:** aggiungere gli utenti EPM Cloud come membri del gruppo. Possono essere aggiunti come membri di un gruppo solo gli utenti assegnati a un ruolo predefinito.
 - a. Fare clic su **Utenti**.
 - b. Cercare gli utenti in **Utenti disponibili**. Per istruzioni, fare riferimento alla sezione [Utilizzo della ricerca](#).
 - c. In **Utenti disponibili**, selezionare gli utenti da aggiungere al gruppo.

- d. Fare clic su **Sposta**.
6. Fare clic su **Salva**.
7. Fare clic su **OK**.


Modifica di gruppi

Gli utenti con ruolo Amministratore servizi possono modificare le proprietà dei gruppi, incluso il nome di un gruppo. L'eventuale modifica del nome di un gruppo non ha alcuna conseguenza sui ruoli applicazione assegnati al gruppo né su altre assegnazioni di sicurezza.

Per modificare i gruppi, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. **Facoltativo:** in **Gestisci gruppi**, individuare il gruppo da modificare. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

Nota: I nomi dei gruppi possono contenere al massimo 71 caratteri. Nell'elenco visualizzato nella colonna **Gruppi disponibili**, tuttavia, compaiono solo i primi 34 caratteri.


3. Fare clic su  (Azione) nella riga del gruppo da modificare, quindi selezionare **Modifica**.
4. **Facoltativo:** modificare il nome del gruppo. La modifica del nome del gruppo non ha alcun impatto sulle assegnazioni di sicurezza effettuate mediante il gruppo.
5. Modificare l'assegnazione dei gruppi.
 - a. **Facoltativo:** aggiungere gruppi nidificati.
 - In **Gruppi disponibili**, cercare i gruppi. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
 - In **Gruppi disponibili**, selezionare i gruppi e fare clic su **Sposta**.
I gruppi selezionati sono elencati in **Gruppi assegnati**.
 - b. **Facoltativo:** rimuovere i gruppi nidificati.
 - In **Gruppi assegnati**, selezionare il gruppo da rimuovere.
 - Fare clic su **Rimuovi**.
6. Modificare l'assegnazione degli utenti.
 - a. Fare clic su **Utenti**.
 - b. **Facoltativo:** aggiungere utenti al gruppo.
 - In **Utenti disponibili** cercare gli utenti che si possono assegnare come membri del gruppo. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

- In **Utenti disponibili**, selezionare gli utenti e fare clic su **Sposta**.
Gli utenti selezionati sono riportati nell'elenco **Utenti assegnati**.
- c. **Facoltativo:** rimuovere utenti dal gruppo.
 - In **Utenti assegnati**, selezionare l'utente da rimuovere.
 - Fare clic su **Rimuovi**.
- 7. Fare clic su **Salva**.
- 8. Fare clic su **OK**.

Eliminazione di gruppi

L'eliminazione di un gruppo non comporta l'eliminazione dei membri che ne fanno parte.

Per eliminare un gruppo, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. **Facoltativo:** in **Gestisci gruppi**, cercare il gruppo da eliminare. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
3. Fare clic su  (Azione) nella riga del gruppo da eliminare, quindi selezionare **Elimina**.
4. Fare clic su **Sì** per confermare l'eliminazione.
5. Fare clic su **OK**.

Importazione delle assegnazioni di utenti a un gruppo da un file

Gli amministratori dei servizi possono importare le assegnazioni di utenti a un gruppo da un file con valori separati da virgole (CSV) per creare nuove assegnazioni in un gruppo Controllo accesso esistente. Oracle Enterprise Performance Management Cloud applica le assegnazioni di sicurezza a livello di applicazione e di artifact in base alle nuove assegnazioni al gruppo.

Nota: Tutti gli accessi utente identificati nel file di importazione devono essere presenti nel dominio identità; tutti i nomi di gruppo inclusi nel file devono essere presenti in Controllo accesso. Non è possibile creare un gruppo utilizzando questo processo di importazione.

È possibile creare solo nuove assegnazioni gruppo; non è possibile rimuovere le assegnazioni gruppo correnti degli utenti.

Nelle illustrazioni seguenti è visualizzato un possibile formato del file CSV di importazione:

```
User Login, Group
jdoe, Example_grp1
jane.doe@example.com, Example_grp2
```

```
User Login, First Name, Last Name, Email, Direct, Group
jdoe, John, Doe, jdoe@example.com, Yes, Example_grp1
jane.doe@example.com, Jane, Doe, jane.doe@example.com, No, Example_grp2
```

Questo formato è identico alla versione CSV del Report gruppo utenti. Se si utilizza questo formato, il processo di importazione ignorerà tutte le colonne tranne Accesso utente e Gruppo. Un modo semplice per creare un file di importazione è esportare il Report gruppo utenti corrente e quindi modificarlo in base alle proprie esigenze. Fare riferimento a [Visualizzazione ed esportazione del Report gruppo utenti](#).

Per importare le assegnazioni di utenti al gruppo, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento alla sezione [Apertura di Controllo accesso](#).
2. Fare clic su **Report gruppo utenti**.
3. Fare clic su **Importa da CSV**.
4. Selezionare il file di importazione utilizzando **Sfoggia** in **Importa CSV assegnazione gruppo di utenti**.
5. Fare clic su **Importa**.
6. Fare clic su **Sì**.

Al termine del processo di importazione verrà visualizzata una finestra di dialogo di conferma nella quale sono indicati il numero totale di assegnazioni elaborate e il loro stato.


Assegnazione di un utente a molti gruppi

Gli utenti di Oracle Enterprise Performance Management Cloud possono essere membri di numerosi gruppi gestiti mediante Controllo accesso.

Per assegnare un utente a molti gruppi, procedere come segue.





1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic su **Gestione utenti**.

Viene visualizzato un elenco di tutti gli utenti dell'ambiente corrente.

3. Cercare l'utente da assegnare ai gruppi. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
4. Fare clic su  (Azione) sulla riga dell'elenco di utenti, quindi selezionare **Modifica**.

Viene visualizzata la schermata **Modifica utente**, nella quale sono riportate le informazioni dettagliate sull'utente, inclusa l'appartenenza corrente ai gruppi (in

Gruppi assegnati). In questa schermata è possibile modificare solo le assegnazioni dei gruppi.

5. Cercare i gruppi da assegnare all'utente. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
6. Completare un'azione tra le seguenti.
 - Per assegnare all'utente altri gruppi, selezionare uno o più gruppi in **Gruppi disponibili** e fare clic su  (**Sposta**) per spostare i gruppi selezionati in **Gruppi assegnati**. In alternativa, fare clic su  (**Sposta tutto**) per spostare tutti i gruppi da **Gruppi disponibili** a **Gruppi assegnati**.
 - Per rimuovere i gruppi assegnati all'utente, selezionare uno o più gruppi in **Gruppi assegnati** e fare clic su  (**Rimuovi**) per spostare i gruppi selezionati in **Gruppi disponibili**. In alternativa, fare clic su  (**Rimuovi tutto**) per spostare tutti i gruppi da **Gruppi assegnati** a **Gruppi disponibili**.
7. Fare clic su **Salva**.
8. Fare clic su **OK**.


Utilizzo della ricerca

La ricerca intelligente di artifact di utenti e gruppi funziona sempre nello stesso modo all'interno di Controllo accesso.

Per trovare specifici utenti, gruppi o ruoli, utilizzare come stringa di ricerca uno degli attributi utente (nome utente, nome, cognome o ID e-mail) oppure il nome del gruppo o il nome del ruolo. Non è necessario utilizzare caratteri jolly nelle stringhe di ricerca. Ad esempio, se si utilizza la stringa `st` per trovare i gruppi, la ricerca restituirà tutti i nomi dei gruppi che contengono la stringa `st`, come `TestGroup`, `Strategic_Planner`, `AnalystsGroup` e così via. Allo stesso modo, se si utilizza la stringa `jd` per trovare gli utenti, la ricerca restituirà l'elenco degli utenti il cui nome utente, nome, cognome o indirizzo e-mail contiene la stringa `jd`.


Nota: Alcune schermate di Controllo accesso, ad esempio, **Assegna ruoli applicazione**, **Report assegnazioni ruoli** e **Report gruppo utenti**, offrono un'opzione di ricerca. Prima di avviare una ricerca, effettuare una selezione appropriata.

Per ricercare utenti, procedere come segue:

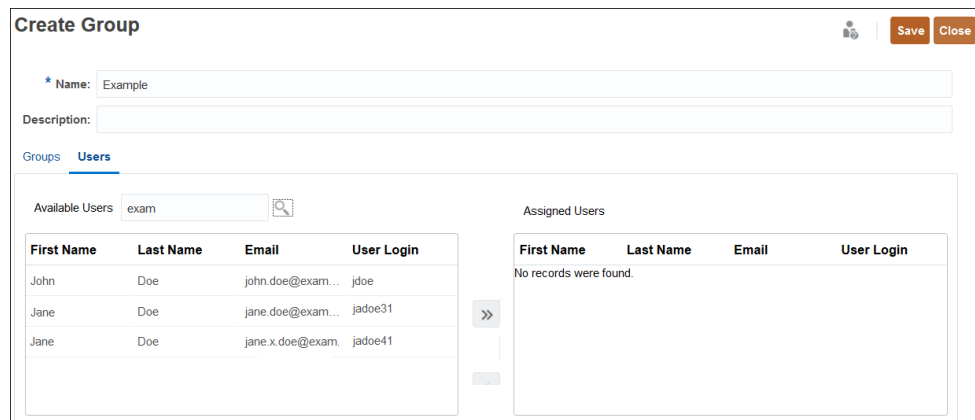
1. Accedere a una schermata, come ad esempio **Gestione utenti**, dove è disponibile la funzione di ricerca.
2. Nel campo di ricerca immettere una stringa parziale di un attributo utente (nome utente, nome, cognome o ID e-mail).
3. Fare clic su  (Cerca).

Nei risultati della ricerca vengono visualizzate tutte le proprietà disponibili per gli utenti che corrispondono ai criteri di ricerca. È possibile ordinare l'elenco facendo clic sull'intestazione di qualsiasi colonna.

Per ricercare gruppi, procedere come segue:

- Accedere a una schermata, come ad esempio **Gestione gruppi**, dove è disponibile la funzione di ricerca.
- Nel campo di ricerca immettere una stringa parziale del nome gruppo.
- Fare clic su  (Cerca).

Nei risultati della ricerca vengono visualizzati il nome e la descrizione dei gruppi che corrispondono ai criteri di ricerca. È possibile ordinare l'elenco dei gruppi recuperati in base al nome o alla descrizione del gruppo.




Create Group Save Close

* Name:

Description:

Groups **Users**


Available Users 

First Name	Last Name	Email	User Login
John	Doe	john.doe@exam...	jdoe
Jane	Doe	jane.doe@exam...	jadoe31
Jane	Doe	jane.x.doe@exam...	jadoe41

Assigned Users

First Name	Last Name	Email	User Login
No records were found.			

Per cercare gli utenti in base ai loro ruoli nel Report assegnazione ruoli, procedere come segue.

- Accedere alla scheda **Report assegnazione ruoli**.
- Selezionare **Utenti** o **Ruoli** nell'elenco a discesa per la ricerca.
- Nel campo della ricerca immettere una stringa da ricercare.
- Fare clic su  (Cerca).

Nei risultati della ricerca vengono visualizzate tutte le informazioni disponibili per gli utenti assegnati ai ruoli che corrispondono ai criteri di ricerca.

Gestione dell'assegnazione dei ruoli a livello di applicazione

L'assegnazione ruoli a livello di applicazione è supportata per le applicazioni Planning, Consolidation and Close, Tax Reporting e Oracle Enterprise Data Management Cloud. Le applicazioni Planning, Consolidation e Oracle Enterprise Data Management Cloud utilizzano ruoli granulari specifici per migliorare l'accesso concesso tramite ruoli predefiniti, mentre l'applicazione Profitability and Cost Management assegna autorizzazioni dati a livello di utente e di gruppo per proteggere l'accesso ai dati dell'applicazione.

Panoramica

Mentre i diritti di accesso complessivi vengono controllati dai ruoli predefiniti di Oracle Enterprise Performance Management Cloud, gli amministratori servizi possono concedere ruoli specifici dell'applicazione e autorizzazioni dati agli utenti e ai gruppi creati e gestiti in Controllo accesso. Ad esempio, per impostazione predefinita un ruolo Utente non dispone del diritto necessario per progettare il processo delle approvazioni. Tale diritto è concesso solo ai ruoli Utente avanzato e Amministratore servizi. In Controllo accesso, gli amministratori del servizio possono assegnare il ruolo Amministratore approvazioni all'utente in modo da consentirgli di eseguire le attività relative alle approvazioni.

L'assegnazione ruoli a livello di applicazione consente di migliorare solo i diritti di accesso degli utenti. Nessuno dei privilegi concessi da un ruolo predefinito può essere ridimensionato dall'assegnazione di un ruolo a livello di applicazione.

Per gestire il processo di assegnazione ruoli si utilizza Controllo accesso. È possibile eseguire i seguenti task:

- Creare gruppi e aggiungere utenti EPM Cloud o altri gruppi come membri.
- Aggiungere o eliminare membri dei gruppi
- Assegnare ruoli delle applicazioni Planning e di consolidamento a gruppi o a utenti
- Visualizzare un elenco di utenti membri di un gruppo

Utenti EPM Cloud

È possibile creare e gestire gli utenti EPM Cloud nel dominio di Identity associato all'ambiente al quale appartiene il processo aziendale. Solo gli utenti assegnati ai ruoli predefiniti possono ottenere i ruoli a livello di applicazione per migliorare l'accesso di cui dispongono al fine di eseguire i task in un processo aziendale.

Ruoli delle applicazioni Planning e Consolidation

I ruoli riportati di seguito possono essere assegnati solo nelle applicazioni Planning, Consolidation e Tax Reporting. Per informazioni sull'assegnazione delle autorizzazioni dati dall'applicazione Profitability and Cost Management, fare riferimento alla guida *Amministrazione di Profitability and Cost Management*.

Per impostazione predefinita, solo gli amministratori del servizio e gli utenti avanzati possono accedere a Gestione dati per intervenire sul processo di integrazione dei dati. Per consentire agli utenti con il ruolo Utente o Visualizzatore del dominio identità di partecipare al processo di integrazione, gli amministrazioni servizi devono assegnare loro i ruoli Gestione dati (Creazione integrazione, Esecuzione integrazione e Drill-through).

Amministratore approvazioni

Risolve i problemi di approvazione assumendo manualmente la proprietà del processo. Comprende i ruoli Assegnatario proprietà approvazioni, Designer processo approvazioni e Supervisore approvazioni.

Di solito, questo ruolo viene assegnato a utenti aziendali responsabili di una regione che hanno l'esigenza di controllare il processo delle approvazioni per la regione, ma che non hanno la necessità del ruolo di amministratore Planning. Possono eseguire i task seguenti:

- Controllare il processo delle approvazioni.
- Eseguire azioni sulle unità di Planning per le quali dispongono di accesso in scrittura.
- Assegnare proprietari e revisori per l'organizzazione di cui sono responsabili.
- Modificare la dimensione secondaria o aggiornare le regole di convalida.

Assegnatario proprietà approvazioni

Esegue tutti i task che possono essere completati dagli utenti con il ruolo Responsabile pianificazione. Inoltre, esegue i task seguenti per qualsiasi membro nella gerarchia dell'unità di pianificazione per la quale l'utente dispone dell'accesso in scrittura.

- Assegnare proprietari.
- Assegnare revisori.
- Specificare gli utenti a cui inviare notifica.

Designer processo approvazioni

Esegue tutti i task che possono essere completati dagli utenti con il ruolo Responsabile pianificazione e Assegnatario proprietà approvazioni. Inoltre, esegue i task seguenti per qualsiasi membro nella gerarchia dell'unità di pianificazione per la quale dispone dell'accesso in scrittura.

- Modificare dimensioni secondarie e membri delle entità per le quali l'utente dispone dell'accesso in scrittura.
- Modificare l'assegnazione di scenario e versione per una gerarchia di unità di pianificazione.

- Modificare le regole di convalida dei dati dei form dati per i quali l'utente dispone dell'accesso.

Supervisore approvazioni

Esegue i task seguenti per qualsiasi membro nella gerarchia dell'unità di pianificazione per la quale l'utente dispone dell'accesso in scrittura, anche se non è il proprietario dell'unità di pianificazione. Questo utente non può modificare i dati nelle unità di pianificazione di cui non è proprietario.

- Arrestare e avviare un'unità di pianificazione.
- Eseguire qualsiasi azione su un'unità di pianificazione.

Creatore di griglia ad hoc

Crea, visualizza, modifica e salva le griglie ad hoc.

Utente ad hoc

Visualizza e modifica le griglie ad hoc ed esegue operazioni ad hoc. Gli utenti ad hoc non possono salvare le griglie ad hoc.

Utente di sola lettura ad hoc

Esegue tutte le funzioni ad hoc, ma non può scrivere nelle griglie ad hoc o caricare dati utilizzando Gestione dati.

Allocazione di gruppo

Esegue le regole di allocazione di massa all'interno delle griglie di form.

Gestione accesso elenco task

Assegna i task ad altri utenti.

Creazione integrazione

Utilizza Gestione dati per la creazione di mapping per integrare i dati tra sistemi di origine e target. Gli utenti possono definire regole dati con varie opzioni di runtime.

Esecuzione integrazione

In Gestione dati esegue regole dati con parametri di runtime e visualizza i log di esecuzione.

Drill-through

Esegue il drill-through nel sistema di origine dei dati.

Ruoli dell'applicazione Oracle Enterprise Data Management Cloud

Questi ruoli possono essere assegnati solo nell'applicazione Oracle Enterprise Data Management Cloud.

Autore applicazioni

Registra le applicazioni in Oracle Enterprise Data Management Cloud. All'utente che registra un'applicazione viene assegnata l'autorizzazione Proprietario applicazione. All'utente viene inoltre assegnato il ruolo di proprietario della vista predefinita dell'applicazione.

Auditor

Visualizza le informazioni relative all'audit, ad esempio la cronologia delle transazioni e le richieste di modifica dei dati in Oracle Enterprise Data Management Cloud.

Autore viste

Crea viste in un'applicazione Oracle Enterprise Data Management Cloud. All'utente che crea una vista viene assegnata l'autorizzazione Proprietario vista per la vista creata.

Assegnazione di ruoli a un gruppo o a un utente


Durante questo processo, gli amministratori servizi assegnano ruoli a livello di applicazione a gruppi e utenti a cui è assegnato un ruolo predefinito.

Nota:

Non è possibile assegnare i ruoli applicazione al proprio account utente.

Per consentire la visualizzazione delle assegnazioni di ruoli, in Controllo accesso i ruoli predefiniti di Oracle Enterprise Performance Management Cloud vengono elencati come gruppi. Non è possibile assegnare loro ruoli a livello di applicazione da Controllo accesso.

Per assegnare ruoli a livello di applicazione a un gruppo o a un utente, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic su **Assegna ruoli applicazione**.
3. Individuare un utente o un gruppo. Nell'elenco a discesa, selezionare **Utenti** o **Gruppi**. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
4. Fare clic su  (**Azioni**) per l'utente o il gruppo, quindi selezionare **Assegna ruoli**.
5. In **Ruoli disponibili**, selezionare i ruoli da assegnare all'utente o al gruppo e fare clic su **Sposta**.

Fare riferimento a queste sezioni per la descrizione dei ruoli che possono essere assegnati a utenti e gruppi.

- [Ruoli delle applicazioni Planning e Consolidation](#)
- [Ruoli dell'applicazione Oracle Enterprise Data Management Cloud](#)


I ruoli selezionati sono elencati in **Ruoli assegnati**. Per rimuovere i ruoli assegnati, selezionare il ruolo da rimuovere in **Ruoli assegnati**, quindi fare clic su **Rimuovi**.

6. Fare clic su **OK**.
7. Fare clic su **OK**.

Rimozione di ruoli a livello di applicazione assegnati a un gruppo o a un utente

Questo processo rimuove tutti i ruoli applicazione assegnati al gruppo o all'utente. La rimozione di un'assegnazione ruolo a livello di applicazione non influisce sui ruoli predefiniti dell'utente.

Per rimuovere i ruoli a livello di applicazione di un gruppo o di un utente, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic su **Assegna ruoli applicazione**.
3. Individuare un utente o un gruppo. Nell'elenco a discesa, selezionare **Utenti** o **Gruppi**. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
4. Fare clic su  (Azioni) per l'utente o il gruppo, quindi selezionare **Annulla assegnazione ruoli**.
5. Fare clic su **Sì**.
6. Fare clic su **OK**.

Generazione di report

Per analizzare e gestire l'assegnazione ruoli utilizzare i report indicati di seguito.

- [Generazione di un Report assegnazioni ruoli per un utente o un gruppo](#)
- [Visualizzazione del Report assegnazioni ruoli per l'ambiente in uso](#)
- [Visualizzazione del Report accesso utenti](#)
- [Visualizzazione ed esportazione del Report gruppo utenti](#)

L'ora di generazione indicata nei report si basa sul formato del fuso orario del browser (clock di sistema locale).

Informazioni sulla versione CSV del report


È possibile esportare un report in modo da creare una versione CSV (Comma Separated Vale, valori separati da virgole) del report. Oltre al numero di utenti assegnati ai ruoli predefiniti, la versione CSV del report fornisce le informazioni riportate di seguito.

- Ruoli predefiniti a cui ciascun utente è assegnato. Ogni ruolo predefinito assegnato a un utente è indicato in una riga separata. I ruoli applicazione inclusi nei ruoli predefiniti non compaiono nell'elenco.
- Ruoli applicazione a cui un utente è assegnato, direttamente o attraverso un gruppo. Ogni ruolo applicazione assegnato a un utente appare in una riga separata.
- I gruppi a cui sono assegnati gli utenti non sono elencati se ai gruppi non è assegnato alcun ruolo.
- Solo le informazioni della vista corrente del report verranno esportate in formato CSV. Ad esempio, se al report si applica un filtro per visualizzare le assegnazioni di ruolo di un utente specifico, il file CSV esportato conterrà solo le assegnazioni di quell'utente.

Generazione di un Report assegnazioni ruoli per un utente o un gruppo

Gli utenti con ruolo Amministratore servizi utilizzano il Report assegnazioni ruoli per esaminare i ruoli predefiniti e i ruoli applicazione assegnati agli utenti. I gruppi a cui un utente appartiene non sono riportati se non sono utilizzati per assegnare ruoli applicazione all'utente stesso. Questo report consente di tenere traccia dell'accesso degli utenti ai fini del reporting per la conformità.

Per generare un Report assegnazioni ruoli per un utente o un gruppo, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic su **Assegna ruoli applicazione**.
3. Individuare un utente o un gruppo. Nell'elenco a discesa, selezionare **Utenti o Gruppi**. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
4. Fare clic su **Azione**  (**Azioni**) per l'utente o il gruppo per il quale generare il report, quindi selezionare **Report assegnazioni ruoli**.
5. **Opzionale:** fare clic su **Esporta in formato CSV** per esportare il report in un file CSV.
6. Fare clic su **Chiudi** per chiudere il report.

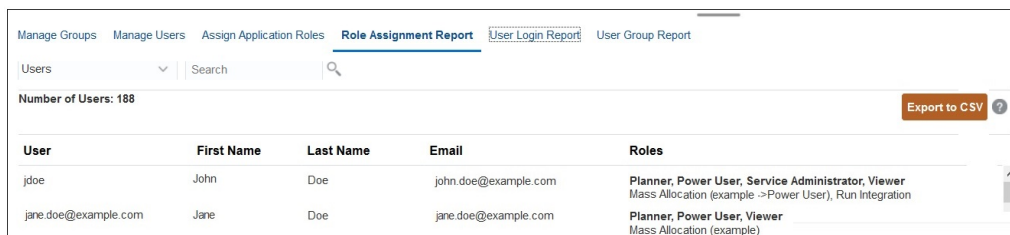
Visualizzazione del Report assegnazioni ruoli per l'ambiente in uso

Gli utenti con ruolo Amministratore servizi utilizzano il Report assegnazioni ruoli per esaminare l'accesso, assegnato tramite i ruoli predefiniti e i ruoli a livello di applicazione, a tutti gli utenti. Il report elenca i ruoli predefiniti, ad esempio Utente avanzato, e i ruoli dell'applicazione, ad esempio Allocazione di massa che è un ruolo dell'applicazione Planning, assegnati all'utente.

I ruoli ereditati, con le informazioni sull'eredità, vengono visualizzati in una riga apposita per ogni utente. Ad esempio, si supponga che l'utente John Doe sia assegnato al ruolo predefinito User e che User sia un membro del gruppo example al quale è assegnato il ruolo Approvals Administrator dell'applicazione Planning. In questo scenario, all'interno delle informazioni sull'assegnazione di ruoli per John Doe, il Report assegnazioni ruoli visualizza quanto segue:

Approvals Administrator (example->User).

Il Report assegnazioni ruoli identifica inoltre il numero di utenti autorizzati ad accedere all'ambiente in base ai rispettivi ruoli predefiniti. Non sono riportati i ruoli dell'applicazione inclusi nei ruoli predefiniti o i ruoli del componente dei ruoli dell'applicazione assegnati all'utente. Per ottenere un report che mostri questi dettagli, è possibile generare la versione classica del report mediante il comando provisionReport di EPM Automate.



The screenshot shows a web interface for the 'Role Assignment Report'. At the top, there are navigation tabs: 'Manage Groups', 'Manage Users', 'Assign Application Roles', 'Role Assignment Report' (active), 'User Login Report', and 'User Group Report'. Below the tabs is a search bar with 'Users' selected and a search icon. A summary line indicates 'Number of Users: 188' and an 'Export to CSV' button. The main content is a table with the following data:

User	First Name	Last Name	Email	Roles
jdoe	John	Doe	john.doe@example.com	Planner, Power User, Service Administrator, Viewer Mass Allocation (example->Power User), Run Integration
jane.doe@example.com	Jane	Doe	jane.doe@example.com	Planner, Power User, Viewer Mass Allocation (example)

È possibile esportare il Report assegnazioni ruoli come file CSV, che può essere aperto con un programma quale Microsoft Excel o salvato sul computer in uso. Il Report assegnazioni ruoli in formato CSV utilizza una riga per ogni assegnazione di ruolo.

	A	B	C	D	E	F
1	User Login	First Name	Last Name	Email	Role	Granted through Group
2	Jdoe	John	Doe	jdoe@example.com	Planner	
3	jdoe	John	Doe	jdoe@example.com	Power User	
4	Jdoe	John	Doe	jdoe@example.com	Service Administrator	
5	jdoe	John	Doe	jdoe@example.com	Viewer	
6	Jdoe	John	Doe	jdoe@example.com	Mass Allocation	example->Power User
7	jdoe	John	Doe	jdoe@example.com	Run Integration	
8	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Planner	
9	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Power User	
10	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Viewer	
11	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Mass Allocation	example

Per aprire il Report assegnazioni ruoli, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento alla sezione [Apertura di Controllo accesso](#).

2. Fare clic su **Report assegnazioni ruoli**.

Verrà visualizzato il Report assegnazioni ruoli.

3. **Facoltativo:** applicare il filtro al report per visualizzare gli elementi indicati di seguito.

- Assegnazioni ruoli di un utente specifico. Selezionare **Utenti** nell'elenco a discesa, quindi immettere una stringa di ricerca parziale. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
- Utenti assegnati a un ruolo specifico. Selezionare **Ruoli** nell'elenco a discesa, quindi immettere il nome parziale del ruolo. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

Nota: È possibile assegnare gli utenti a molti ruoli. In tali casi, nel report vengono elencati tutti i ruoli dell'utente anche se il filtro è per un ruolo specifico.

4. **Opzionale:** fare clic su **Esporta in formato CSV** per esportare il report in un file CSV. Si noti che in formato CSV vengono esportate solo le informazioni del report correntemente visualizzato.

Visualizzazione del Report accesso utenti

Per impostazione predefinita, il Report accesso utenti contiene informazioni sugli utenti che hanno effettuato l'accesso all'ambiente nelle ultime 24 ore. Il report elenca l'indirizzo IP del computer da cui l'utente ha effettuato l'accesso e la data e l'ora (UTC) in cui l'utente ha effettuato l'accesso all'ambiente.

Gli amministratori del servizio possono generare di nuovo questo report per un intervallo di date customizzato oppure per gli ultimi 30 giorni, gli ultimi 90 giorni e gli ultimi 120 giorni. Possono inoltre applicare un filtro al report per visualizzare solo le informazioni di utenti specifici utilizzando come stringa di ricerca una stringa parziale del nome, del cognome o dell'ID utente dell'utente.

Nota: In Oracle Enterprise Performance Management Cloud la cronologia di audit degli accessi utente viene conservata solo per gli ultimi 120 giorni.

Per generare un report sugli accessi utente, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic su **Report attività accesso utenti**.

Viene visualizzato un report in cui sono elencati tutti gli utenti che hanno effettuato l'accesso all'ambiente nell'ultimo giorno.
3. Selezionare un periodo, ad esempio Ultimo giorno, Ultimi 30 giorni, Ultimi 90 giorni o Ultimi 120 giorni, in base al quale generare il report. Per specificare un intervallo di date customizzato, selezionare **Intervallo date**, quindi selezionare una data di inizio e una di fine.
4. **Facoltativo**: selezionare gli utenti da includere nel report. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
5. **Facoltativo**: fare clic su **Esporta in formato CSV** per esportare il report visualizzato in un file CSV.
6. Fare clic su **Annulla** per chiudere il report.

Visualizzazione ed esportazione del Report gruppo utenti

Nel Report gruppo utenti è indicata l'appartenenza, diretta o indiretta, degli utenti assegnati ai gruppi in Controllo accesso.

Gli utenti che sono assegnati a un gruppo, ne sono automaticamente membri diretti; sono considerati membri indiretti se sono assegnati a un gruppo che è un figlio di un altro gruppo. Per ogni utente assegnato a un gruppo, nel report sono fornite informazioni quali ID di accesso, nome e cognome, ID e-mail e un elenco separato da virgole dei gruppi ai quali l'utente è assegnato direttamente o indirettamente. Nella versione CSV del report è indicato se l'utente è assegnato direttamente o indirettamente a un gruppo tramite la dicitura SÌ o NO.

Nota: Questo report non è applicabile ad Account Reconciliation e Narrative Reporting.

Per rigenerare il Report gruppo utenti, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic su **Report gruppo utenti**.
3. **Facoltativo**: applicare il filtro al report. Nell'elenco a discesa, selezionare **Utenti o Gruppi**. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
4. **Opzionale**: fare clic su **Esporta in formato CSV** per esportare il report in un file CSV.
5. Fare clic su **Annulla** per chiudere il report.